EJT

Research Article

SECURITY IMPROVEMENTS OF INTERNET OF THINGS SYSTEMS

Fouad A. ABDULKAFI*[1]*, Sefer KURNAZ*[1]*, Ayad A. ABDULKAFI*[2]**

In this paper, we discuss the security of the Internet of Things (IoT) which needs to utilize particular algorithms in order to offer low power consumption and a long lifespan, along with other parameters such as strong immunity against attacks, lower execution time and acceptable performance. The present work considers a simple lightweight security encryption algorithm (LSEA) to be compatible with IoT systems, named (LSEA-IoT) for improving the security issue in IoT devices. The new LSEA-IoT scheme has be implemented for encrypting texts and images data and several tests such as visual checking, histogram diagrams, entropy and correlation analyses are carried out in order to ensure the suitability of the LSEA algorithm. Simulation results show that the performance of LSEA based IoT scheme achieves acceptable security level in terms of histogram, entropy and correlation performances as well as it has a good execution time performance for different types of messages. Based on this analysis, it can be concluded that the proposed LSEA-IOT is a promising algorithm and can be considered as an appropriate nominee to be utilized for IoT devices and it can be used for real-time applications.

Key words*: IoT, Security, Encryption, LSEA*

1. Introduction

The information and communications technology (ICT) systems have grown significantly in different areas due to their platforms provide faster information exchange, cost reduction and increasing productivity. A recent concept raised called the Internet of Things (IoT), assuming all “things” will be connected to popular internet via ting equipment with telecommunication systems. Many software, devices, services and connectivity are involved in IoT technology. Based on data and analytics global data company, IoT reached 130 billion dollars in 2018 and it is expected to reach 318 billion dollars with a compound annual growth rate (CAGR) of 20% by 2023 as can be seen in Fig. 1 [1]. In such scenario, anything is allowed to communicate to everything which makes life easier for everybody. IoT devices can be connected using cars, washers, lights, watches, helmets, ropes, forks, pacifiers and even socks. At the moment, we are in the process of connecting everything to the IoT, whether IoT facilitates the life or not. The main issue of IoT technology at current time is the data gathering and analyzing the

[1]Department of Electrical and Computer Engineering, Altinbas University, Istanbul, Turkey, (sefer.kurnaz@altinbas.edu.tr) https://orcid.org/0000-0002-7666-2639

[2]Department of Electrical Engineering-Shirqat, Tikrit University, Salahaddin, Iraq, (ayad_atiyah@tu.edu.iq) https://orcid.org/0000-0002-1160-6011

Received: 12 March 2020; Accepted: 5 July 2020 Doi: https://doi.org/10.36222/ejt.702563

collected data in a useful and correct manner. As the connections between things and the Internet is ensured, several insights into life and environment will be gained.

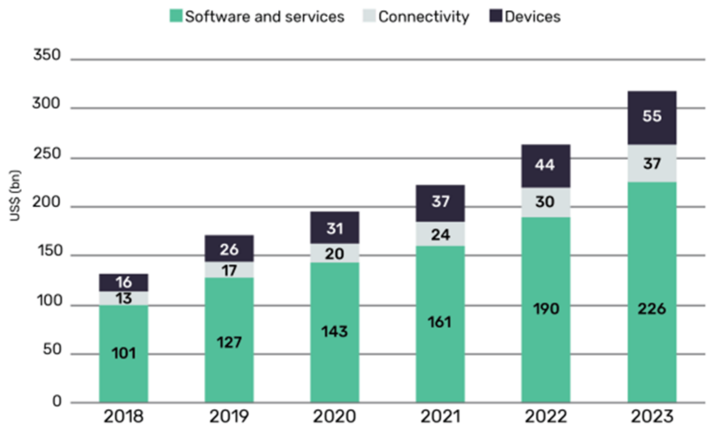


Figure 1. IoT market size for 2018-2023 [1].

For instance, it is possible to allow others to obtain the similar insight if security issue cannot be handled correctly. As a sequence, securing the IoT devices is become a hotspot of research area and even an important topic in near future because the envisioning of more things assumed to be connected to the IoT [2].

2. Cryptographic algorithms based IoT related works

The This part presents some literatures related to the cryptographic techniques. The properties of these techniques and how they can be utilized for securing the connections between IoT devices to perform the encryption protocol are also presented in this paper. The rudimental cryptographic which is a basic mathematical model can be jointed with other primitives to build cryptographic protocols, also known as cryptosystems. The primary familiar cryptographic consist the encryption algorithms, protocols of key agreement, PN generators and cryptographic hash functions.

The work in [3] has suggested a hybrid scheme for encryption to reduce risks in safety and improving the speed and complexity of encryption algorithms. The aim is to focus on information confidentiality, integrity, non-rejection for exchanging data in IOT. The proposed algorithm has been assessed in terms of speed, and security efficiency using MATLAB and compared to the traditional encryption algorithms. Another scheme to build secure service form via semantic security policy is provided in [4]. They defined and matched the algorithm of semantic security algorithm by implementing universal ontology of security as well as adopting modelling tools as competitor ontology along with semantic reasoner to implement this prototype.

More general view on IoT growth and computing beside to use the machine learning (ML) methods to secure, for example, the traffic flow and the equipment employed in IoT applications with fog computing systems can be found in [5-6]. Authors in [5] have surveyed methods used to determine attacks and detect the abnormalities using the ML techniques along with engineering solutions for IoT data growth and dictates more studies on security problems related to fog computation. As a result of IoT commercialization, more security concerns have been raised by individuals and publics such as personal privacy subjects, cyber threat attacks as well as organized offenses. The IoT has three layers which include the edge nodes, communication and edge computing. The work in [7] has investigated the security of IoT applications through reporting a comprehensive study of the weak points and actions required on the edge-side layer of IoT with a description of potential countermeasures to avoid attacks.

More recently, the study [8] discussed the shortcomings of available studies and provided a detailed assessment for different methods related to the most important subjects of security, privacy issues. Their work transferred the meaning of smart M-IoT system from its concept and ideology. The works also covered the IoT devices and corresponding applications, possible advances and existed challenges along with properties and technologies. The emerging security threats issues have been presented in [9] highlights the structure defects of mobile devices and human mistakes and underlines the vulnerabilities in traditional algorithms. As a result, methods have been suggested based on each category find solutions against emerging attacks as well as providing a comparison with the existing solutions.

Based on software-defined network (SDN) architecture, the authors in [10] have proposed a new security architecture for wired and wireless systems. The disused model consists of Ad-Hoc network and reticular things such as sensor objects, tablet and smartphones. The SDN architecture can extend the security to access the network. Meanwhile, the study in [11] has combined two methods, which are the advanced encryption standard (AES) and elliptic curve cryptosystems (ECC) algorithms for ensuring the security in IOT systems. It is worth to mention that earlier to above, the work in [12] has introduced the standard IP-based security framework as a security solution aiming to provide the best IoT optimization via the combination of end to end and public key cryptography. Resolving the security challenges in IOT has been presented in [13] for preventing the exporter’s security flaws. In this way, after taking the related issues, owner has to export them to access devices with oval ECDSA elliptically algorithm. In [14], a public key cryptographic algorithm based on elliptic curves called SM2 encryption algorithm. SM2 is an innovative way to research on the security of IOT and used as a security framework to tackle issue between user end and reception side when transmitting the information between them.

The SM2 algorithm has been executed via a large range of elliptically graph of ECC based IOT. The work presented in [15] introduced a systematic method consists of individual, process, technological ecosystem and smart thing nodes. The security of the proposed approach is based on the strategy, used standards, trends and policy evidence documents. Another framework for security for 4G networking has been discussed in [16] to demonstrate the challenge of IOT security. It aims to improve speed of IoT communication which enables the client for accessing the available resources in 4G networks. On the other hand, the framework in [17] has dedicated to secure the embedded safety of IOT for both software and hardware using the MAC protocol in physical and MAC layers. Blowfish method based on the field-programmable gate array (FPGA) and Verilog Hardware Description Language (VHDL) has supervision on the used resources in FPGA [18]. In Fact, Blowfish algorithm considered as a good choice for improving the IoT security performance. In addition, the Hash algorithm has been proposed to improve the security when transmitting messages in smart homes [19]. Moreover, reducing the risks in valuable applications was the main goal of the study presented in [20] to fit system management utilizing a hybrid algorithm for encryption process. The hybrid scheme is implemented based on Data Encryption Standard (DES) and the Digital Signature Standard (DSA) algorithms. The key technologies for the IoT based on radio frequency identification (RFID), code identification and electronic technologies are presented in [21] to show the usage of these keys in digital form of agricultures. The work in [22] has introduced another hybrid system for encrypting the messages using the DES and Rivest-Shamir-Adelman (RSA) algorithm in Bluetooth applications. A survey performed on lightweight encryption algorithms, technologies, and architectures in IoT can be found in [23].

3. System descriptions

3.1. System model

The block diagram of the proposed scheme is shown in Fig. 2. The proposed lightweight security encryption algorithm (LSEA) is based on a block cipher with symmetric key using 64-bit key to encrypt the plaintext messages. LSEA scheme generates diffusion and confusion to improve the IoT security though the encryption operation. This process has many rounds, each encryption round consists a set of mathematical equations. As the number of rounds increased, improvements in security can be obtained on the expense of increasing in energy consumptions. Most encryption processes are implemented with 20 rounds or more rounds to ensure strong security to satisfy the system requirements. The proposed LSEA algorithm has no more than five rounds which means more saving in power consumption and enhances the system efficiency. Every round of encryption consists of mathematical functions that executed with four data bits. The used functions in LSEA are capable to generate more confusion and diffusion in data messages that result in confronting the potential attacks with the Feistel connection networks.

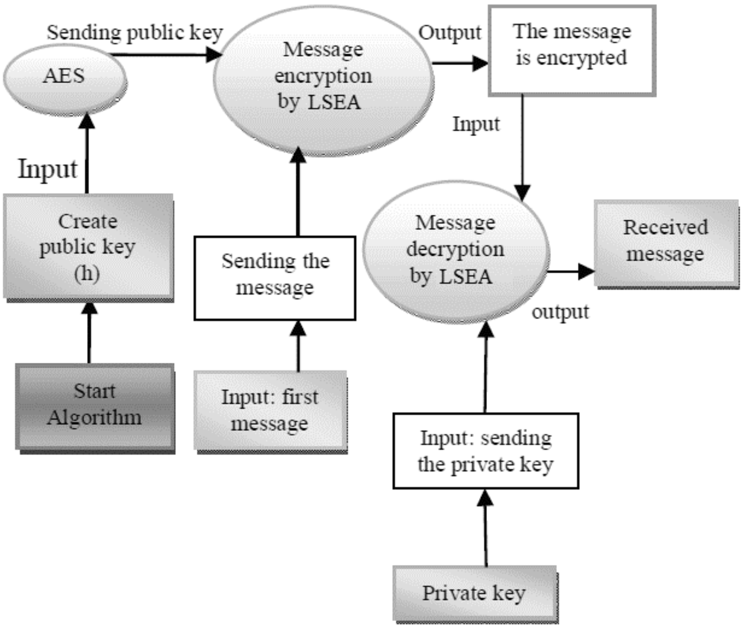


Figure 2. Proposed LSEA-IoT block diagram.

3.2. Key generation

The most important process in encryption and decryption is the generation of key. Key generation ensures the data security and makes it dependent because if the attacker knows the key, the data's secrecy will be in risk and lost. For this, attentions should be given to make sure that knowing the key by the third parity or attacker as difficult as possible. To achieve this purpose, for example, the encryption algorithm based on Feistel network contains many rounds and each round needs a separate and different key. In this research, encryption process and/or decryption operation include five rounds; hence, there is a need to create five unique keys to perform this task. This purpose requires a block to expand the key as will be discussed later in this section. Similar steps are followed in AES to create the required key. Two 4 x 4 matrices are employed to create encryption key. A specific location in state matrix and a predefined key is chosen from the key matrix. These are randomly chosen in order to generate the public key (h) using logic operation of XOR gate based hexadecimal basis. The goal is to transmit a hidden data of transmitter to the desired receiver. In this way, only the receiver knows and can recognizes the private key while both transmitter and receiver know the public key [3].

Therefore, the encryption operation must have a strong security. For this reason, the encrypted information data at the sender is transmitted to the receiver in secure way and good safety. Therefore, the proposed LSEA encryption can improve the security as transmitted data message has been sufficiently encrypted and can be estimated by the intended receiver only. It is worth to mention that the key generation architecture can not support different key length and rely on the processed data.

3.3. Encryption process

The flowchart of the proposed algorithm with its details can be seen in Fig. 3. When the data is transmitted from the information source to the receiver, the sender randomly selects a multi nominal like r from the collection like L_r. Therefore, it must not be revealed by the transmitter or sender. The encryption process for a message (M) can be expressed as [23].

$$E \ = P_r * \ h + M \qquad (1)$$

Where P_r represens the private key and the information is transmitted to the intended side as an encrypted data **(**E) with the required capability of security using the first generated public key (h) (see appendix for mathematic analysis).

3.4. Decryption process

As the message has been encrypted, the receiver attempts to decrypt the message using its private key in order to extract the message. The receiver has to know the following keys *f* and f_p (private keys). it is worth to mention that f_p is a multinomial conversion of *f*, so that *f* multiplied by fp is equal to one. The intended receiver has to multiply the received data message by a part of private key which is indicated by parameter *a* as can be written below [23]

$$a = f * E = f * (P_r * \ h + M) = (f * P_r * \ h + f * M) = f * M \qquad (2)$$

Where $P_r * \ h = 0$ as it completely reduced and have no any impact on the operation. The receiver has to do the decryption process (D) to estimate the original message ($\ddot{M}$). The decryption process (D) can be expressed as:

$$D = \frac{fp*a}{x^2} = \frac{fp*f*M}{x^2} \cong \ddot{M} \qquad (3)$$

In fact, the decryption is the reverse operations done at the encryption process. In general, the assumed public key can be used for encryption process while the private key is used for both encryption and decryption.

4. Evaluation parameters

The following parameters are used to evaluate the proposed model for securing the IoT systems.

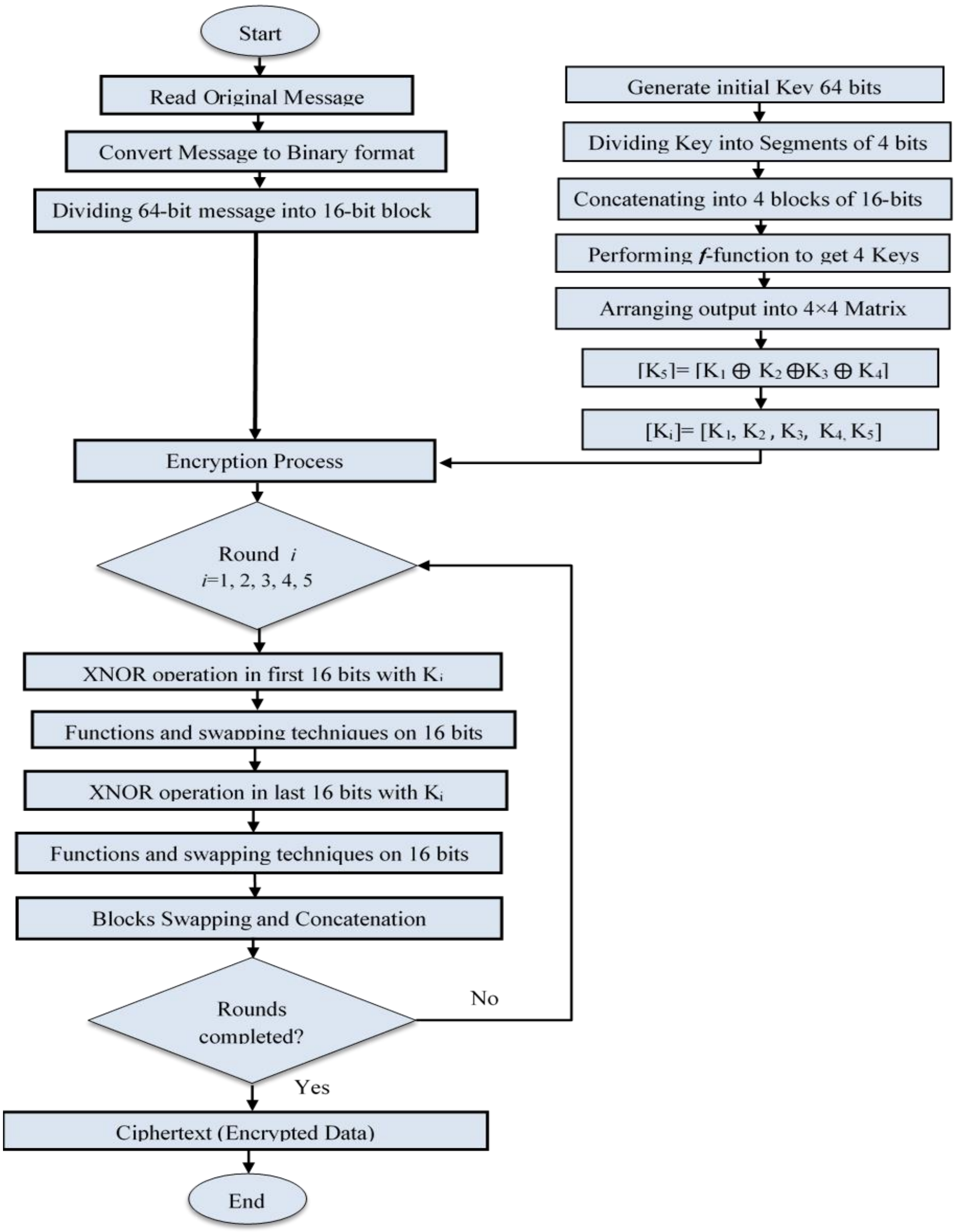

Start
Read Original Message
Convert Message to Binary format
Dividing 64-bit message into 16-bit block
Generate initial Key 64 bits
Dividing Key into Segments of 4 bits
Concatenating into 4 blocks of 16-bits
Performing f-function to get 4 Keys
Arranging output into 4×4 Matrix
[K5]= [K1 ⊕ K2 ⊕K3 ⊕ K4]
[Ki]= [K1, K2 , K3, K4, K5]
Encryption Process
Round i
i=1, 2, 3, 4, 5
XNOR operation in first 16 bits with Ki
Functions and swapping techniques on 16 bits
XNOR operation in last 16 bits with Ki
Functions and swapping techniques on 16 bits
Blocks Swapping and Concatenation
Rounds completed?
No
Yes
Ciphertext (Encrypted Data)
End

Figure 3. Flowchart of LSEA Algorithm.

4.1. Entropy

The IoT systems utilize the encryption algorithms for ensuring the required security. However, these algorithms add extra bits to the information data therefore it must be not possible for an attacker to distinguish between the message plaintext and the encrypted data by these algorithms. The information amount contained in messages can be measured using the entropy metric. The entropy is associated to the relative degree of randomness. Generally, high value of the entropy means thigh level of randomness. Consequently, as entropy is higher, the performance of security algorithm is better. For instance, entropy (*H*) for an image message, Shannon formula can be applied on values of image intensity (*I*) and corresponding values of probability of intensity *P*(I_i) [24].

$$H(I) = -\sum_{i=1}^{2N} P(I_i) log_b\, P(I_i) \qquad (4)$$

If the sender source generates 256 symbols (2^8) with same probabilities and $s = \{s_1, s_2, . . ., s_{2^8}\}$, the result entropy should be equal to eight. However, as encryption algorithms almost generate symbols and their entropy will be less than eight, it is possible to estimate message data from the encrypted message, which considered as a risk to the safety of devices in IoT network.

4.2. Correlation analysis

Consider a pixel that associates with neighbouring pixels in the original message image. The adjacent pixels are correlated in horizontal, vertical, and diagonal orientations. This correlation can be represented by the following equations [25].

$$R_{xy} = \frac{Con(x,y)}{\sqrt{D(x)}\,\sqrt{D(y)}} \qquad (5)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_j - \frac{1}{N}\sum_{i=1}^{N} x_j\right)^2 \qquad (6)$$

$$Con(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_j - \frac{1}{N}\sum_{i=1}^{N}(x_j\right)\left(y_j - \frac{1}{N}\sum_{i=1}^{N}(y_j)\right) \qquad (7)$$

where, r_{xy} refers to the coefficient of correlation. Variables x and y represent the intensity values of two adjacent pixels in the image while the number of pair pixels of the chosen adjacency in the data image is denoted by N to determine the correlation. The ideal coefficients of correlations of original message should be equal to 1 while for encrypted image, these correlation coefficients must be equal to zero. At the beginning, identifying the neighbourhood of horizontal, vertical, and diagonal of N pixels has to be performed. Later, histogram is drawing according to each pixel value and its neighbours.

In addition, there are two common measures are employed for the analysis which are the NPCR and UACI [23]. NPCR can be defined as the number of pixels change rate of the encrypted message when changing one pixel of the original message (image). The unified average changing intensity (UACI) is used to measure the average intensity of the differences between the original message and the encrypted one.

4.3. Execution time

One of the important parameters for the assessment of algorithms is its time that will be taken for encoding and decoding a specific data. While the proposed method is dedicated for the IoT devices, it should take time as minimum as possible while offering considerable and accepted security.

5. Results and discussion

In this section, simulation results of the proposed LSEA performance are discussed. The framework of the LSEA approach is simulated to execute the standard evaluation metrics such as entropy and histogram of image using Intel Core i5-6200U@ 2.30 GHz processor using MATLAB software. The simulation also observes the utilization in memory and execution time of the proposed scheme.

The simulation results shown in Fig. 4 demonstrate that the correct decryption can be achieved only when using the correct key for decrypting the message image, otherwise the original data cannot be recovered. For a clear illustration, the avalanche test is also performed by using bit from the original key create the wrong key, the power of the proposed method can be observed from this analysis. To do the tests of entropy and histogram analysis, the popular 8-bits grey scale Lena image has been selected. It is clear that the original message can be successfully extracted via decrypting the received messages using the proposed algorithm. The image histogram is considered as a tool to visually check effect of the encryption algorithm of an image using LSEA algorithm. In addition, this test is used to observe and evaluate the randomness produced in the image. To assess the produced randomness, the histogram of the image is performed. In order to depict the appreciable LSEA security, a uniform histogram has been done after the encryption process. It is known that for huge sets of data, using the histogram is better in displaying the distribution of data than other plots such as leaf and stem plots.

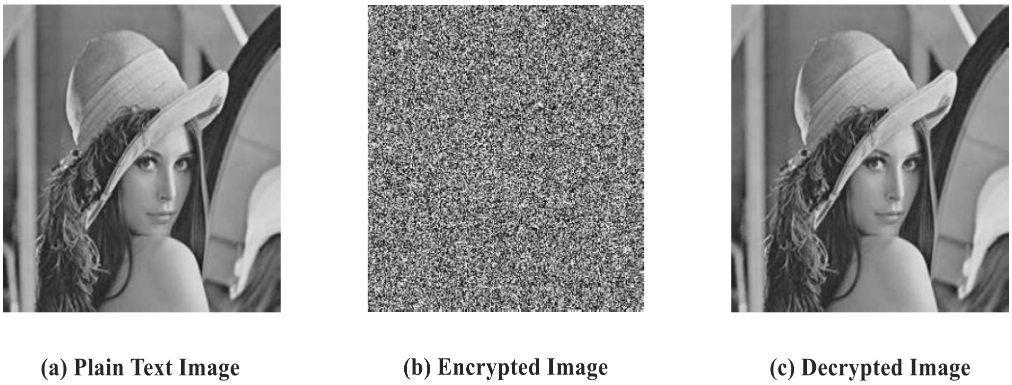
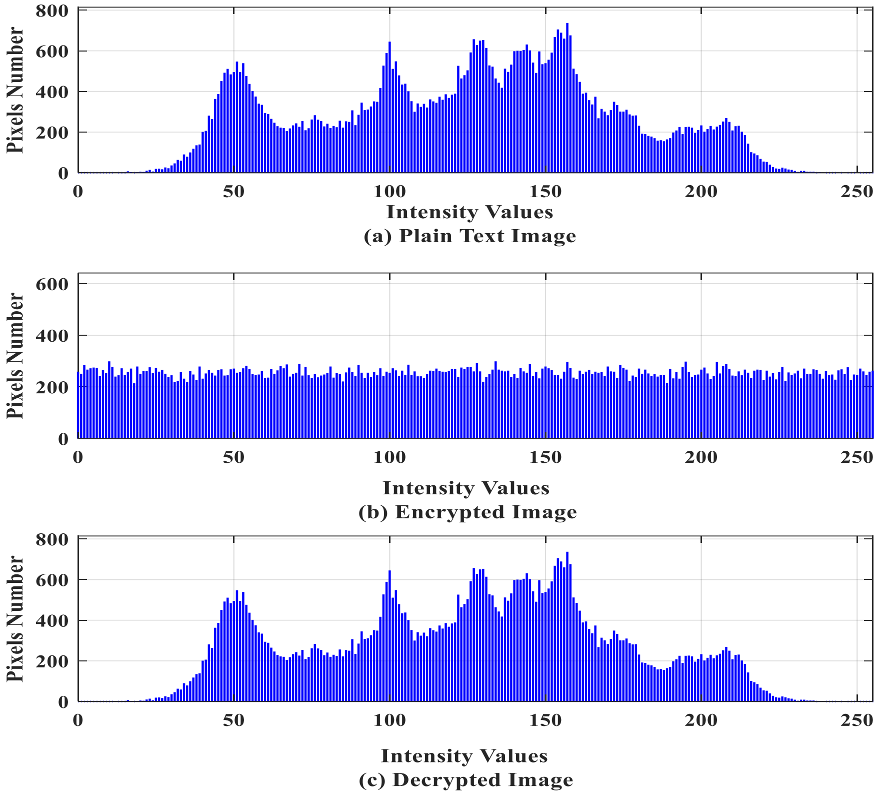


Figure 4. Encryption/Decryption of Lena Image using LSEA.

The histogram performance in terms of pixel number versus the intensity values for different at different stages is investigated. Histogram of the 8-bits grey scale before and after applying the proposed LSEA model on popular Lena image is illustrated in Fig. 5. The proposed LSEA algorithm is applied and the histogram results are obtained for three phases, i.e. for original image, encrypted image and for the decrypted image. It is clear that the resulted uniform distribution of intensity of encrypted image predicts and provides a clear pointing of required security of LSEA scheme.

In order to avoid the leakage of information and hard attacks, it is necessary to ensure that the original message and encrypted message images do not have any statistical similarity. Hence, using the histogram analysis that shows the pixels distribution of an image through the drawing number of observations of the amount of brightness for each pixel. Figure 5 demonstrates the histogram metric on the image tested using LSEA algorithm. It is clear, the histograms of plain text message and decrypted image have sharp rises with a sharp declines as can be seen in Fig. 5(a) and Fig. 5(c), while the histogram of the encrypted image has a uniform distribution (see Fig. 5(b)) that is totally different when comparing to the histogram of the decrypted and original image and hence no observation of statistical similarity is noticed. For this, it is difficult for the potential attacker to acquire the information using the histogram of the image after encrypting it using LSIA algorithm.

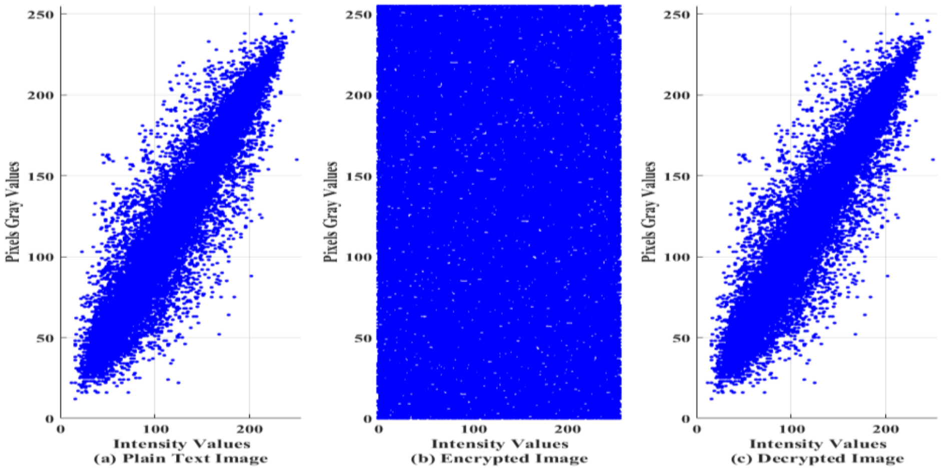


(a) Plain Text Image

(b) Encrypted Image

(c) Decrypted Image

Figure 5. Histogram of Images at different stages.



(a) Plain Text Image

(b) Encrypted Image

(c) Decrypted Image

Figure 6. Correlation comparison of an Image at different stages.

Figure 6 demonstrate the contrast between original, encrypted and decrypted image data. Original plaint text image is seen to be highly associated and has a high value of correlated contained in its coefficient. On the other hand, the encrypted data image seems to have no correlation depicting the strength to the proposed algorithm. As can be seen in Fig. 6, the correlation between pixels of the original plain text image is very high, while the correlation between the neighbouring pixels in the encrypted image is very small. Moreover, Tab 1 shows the correlation coefficients of the original, encrypted and decrypted images by the proposed encryption methods for the diagonal, vertical and horizontal neighbourhoods. It can be seen from this table that the correlation coefficients values of the algorithm are around zero for each neighbourhood. Consequently, the LSEA algorithm can be considered as a secure against correlation attacks. It is found that the absolute values of the NPCR between the encrypted and original message image is equal to 99.5972 while the UACI is about 14.8724. The high values of NPCR and UACI show that the proposed LSEA encryption algorithm has a high sensitivity to the original message.

Table 1. Correlation and Entropy of for original, encrypted and decrypted Lena Image

Algorithm	Parameter	Original Image	Encrypted Image	Decrypted Image
LSEA	Correlation	0.995972	0.148724	0.995972
	Entropy	7.4509	7.9969	7.4509
Related work [3]	Correlation	0.9744	0.12	None
	Entropy	7.4504	7.9973	None

Table 2: Comparison between proposed algorithm and related algorithms

Algorithm	Block Size	Key Size	Round Number	Computational time (second) in MATLAB Environment
AES	128	128	10	65.23
DES	64	56	16	56
LSEA	64	64	5	46.398

From Tab 2, it appears clearly that the proposed algorithm is better than the others. Indeed, it offers the smallest execution time for both encryption and decryption for the same data size. The execution time taken by the algorithm is explained by the fact that in each step of the encryption and decryption is performed only on five rounds.

Finally, the execution time of the proposed LSEA algorithm in in MATLAB programming environment which cover both the encryption and the decryption execution time has been evaluated in this work. Each of these will be measured across the time to encrypt or decrypt a file of a certain size for different message types and formats. Fig. 7 shows the total time needed for encryption for different message types using the proposed LSEA. As it is expected, the text messages have the lowest encryption time compare with image messages. It is worth to mention that all messages have the same size of original data file which is equal to 9 Kbit. Moreover, it can be seen that image with extension of BMP has less encryption time than other images types. On the other hand, the JPG requires more time to encrypt the image compare with other formats.

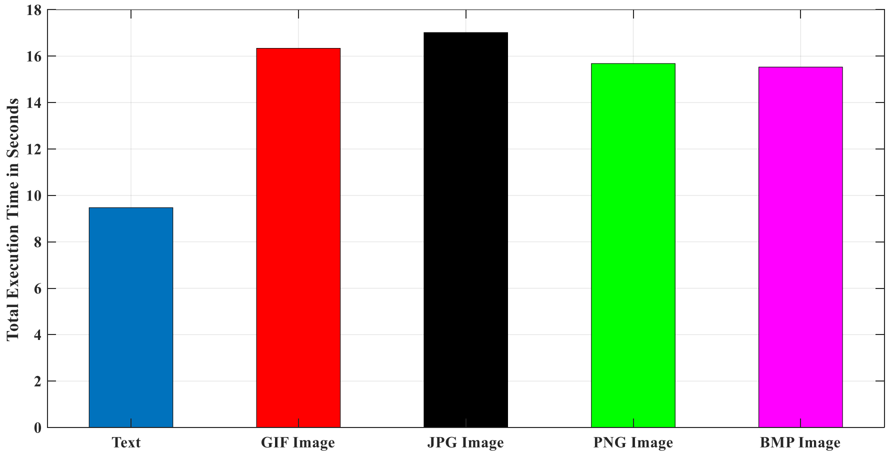


Figure 7. Total Execution Time for different Message Types using LSEA-IoT.

6. Conclusion

A light encryption algorithm for securing the IoT devices and systems is proposed in this research paper. Several statistical tests are carried out to prove the validity and suitability of the proposed LSEA algorithm for IoT applications. The security scheme for IoT based on the proposed algorithm encrypts messages using two keys, i.e. private and public keys. Simulation results demonstrate the accurate encryption and decryption processes and the histogram is used to show the effect of the LSEA encryption algorithm to observe the randomness produced in the image. It has been shown that histograms of the encrypted, decrypted and original image have no statistical similarity and hence it is difficult for the potential attacker to acquire the required information. In addition, it is found that encrypted data have no correlation depicting the strength to the proposed LSEA algorithm. The obtained NPCR and UACI values have proved the high sensitivity of the proposed LSEA encryption algorithm. In order to further improve the performance of LSEA-IoT scheme, future works on strengthening the generated key via specific processing with PN codes can be investigated along with their effect on other evaluation parameters of the proposed algorithm. Moreover, although the proposed algorithm is restricted to just five pounds only which reveals low cost, but a deeper cost analysis is left to a future study.

References

[1] https://www.windpowerengineering.com/business-news-projects/global-iot-market-to-reach-318-billion-by-2023-says-globaldata/, 2018.

[2] Tuen, Christian Dancke. "Security in Internet of Things Systems." MSc thesis, NTNU, 2015.

[3] Yousefi, Afsoon, and Seyed Mahdi Jameii. (2017). Improving the security of internet of things using encryption algorithms. *In 2017 Int. Conference on IoT and Application (ICIOT*), 1-5.

[4] Zhengqiu, H, Xue F, Liu W, He R, and Xu Z. (2016). Research of Secure Service Composition Based on Semantic Security Policy. *IEEE International Conference on Internet of Things (iThings) and Green Computing and Communications (GreenCom) and Cyber, Physical and Social Computing (CPSCom) and Smart Data (SmartData)*, 246-251.

[5] Moh, Melody, and Robinson Raju. (2018). Machine Learning Techniques for Security of Internet of Things (IoT) and Fog Computing Systems. *IEEE International Conference on High Performance Computing & Simulation (HPCS)*, 709-715.

[6] Sönmez, Yasin, Hüseyin Kutlu and Engin Avci. (2019). A novel approach in analyzing traffic flow by extreme learning machine method. *Tehnički vjesnik*, 26(1), 107-113.

[7] Mosenia A. and Niraj K. Jha. (2016). A comprehensive study of security of internet-of-things. *IEEE Transactions on Emerging Topics in Computing*, 5(4), 586-602.

[8] Sharma, V., You, I., Andersson, et. al. (2020). Security, privacy and trust for smart mobile-Internet of Things (M-IoT):A survey. *IEEE Access*, 8(2020), 167123-167163.

[9] Su, X., Wang, Z., Liu, X., Choi, C. and Choi, D. (2018). Study to improve security for IoT smart device controller: drawbacks and countermeasures. *Security and Communication Networks*.

[10] F. Olivier, G. Carlos, N.Florent . (2015). New Security Architecture for IoT Network. *Procedia Computer Science*, 52, 1028-1033.

[11] M.Xin, H.China.)2015). A Mixed Encryption Algorithm Used in Internet of Things Security Transmission System. *IEEE International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, Xian, 62-65.

[12] H.Shafagh, A.Hithnawi. (2014). Poster Abstract: Security Comes First, A Public key Cryptography Framework for the Internet of Things. *IEEE International Conference on Distributed Computing In Sensor Systems (DCOSS)*, Marina Del Rey, CA, 135-136.

[13] A.F.Skarmeta, J., M M. (2014). A decentralized approach for Security and Privacy challenges in the Internet of Things. *IEEE Word Forum on Internet of Things (WF-IOT), Seoul*, 67-72.

[14] N.Hong, Z.Xuefeng. (2013). A Security Framework for internet of things based on SM2 cipher algorithm. *Fifth IEEE International Conference on Computer Science and Network Technology*, Shiyang, Hubia, China, 13-16.

[15] R. Arbia, Y. Challal, E.Natalizio, Z.Chtourou, and A. B. (2013). A systemic approach for IoT security. *IEEE International Conference on Distributed Computing in Sensor Systems*, 351-355.

[16] L.yuan Zeng. (2012). A Security Framework for Internet of Things Based on 4G communication. 2*nd IEEE International Conference On computer Science And Network Technology,* Chanchun, China, 1715- 1718.

[17] S. Babar, A.Stango, N.Prasad, J.Sen, R.Prasad. (2012). Proposed embedded security framework for internet of things. *2nd IEEE International Conference on Information Theory and Aerospace & Electronics Systems Technology*, Chennai, 1-5.

[18] K.Nur Prasetyo ST, Y. Purwanto, and D. Darlis. (2014). An implementation of data encryption for Internet of Things using blowfish algorithm on FPGA. *2nd IEEE International Conference Information and Communication Technology (ICoICT),* Bandung, 75-79.

[19] SB. Vinayaga, M. Ramnath, M. Prasanth, and V. Sundaram. (2015). Encryption and hash based security in Internet of Things. *3rd International Conference Signal Processing, Communication and Networking (ICSCN),* Chennai, 1-6.

[20] P.Xu, Li .Min, and He. Yu-Jie. (2013). A hybrid encryption algorithm in the application of equipment information management based on Internet of things. *In 3rd International Conference on Multimedia Technology (ICMT-13).* Atlantis Press, 2013.

[21] X. Yi Chen, Zh.Gang Jin. (2012). Research on Key Technology and Applications for Internet of Things. *Physics Procedia*, 33, 561-566.

[22] R.Wuling, and Zh. Miao. (2010). A hybrid encryption algorithm based on DES and RSA in Bluetooth communication. *2nd IEEE International Conference on Modeling, Simulation and Visualization Methods (WMSVM),* Sanya, 221-225.

[23] Sharma, T. P. (2020). Lightweight Encryption Algorithms, Technologies, and Architectures in Internet of Things: A Survey. *Innovations in Computer Science and Engineering*, 341-351.

[24] Safi, Amirhossein. (2017). Improving the security of Internet of things using encryption algorithms. *Int J Comput Electr Autom Control Inf Eng*. 11(5), 546-549.

[25] C. E. Shannon. (1949). Communication theory of secrecy systems. *Bell Systems Technical Journal*, 28, 656–715.

[26] S. S. Agaian, R. G. R. Rudraraju, and R. C. Cherukuri. (2010). Logical transform-based encryption for multimedia systems. *In Proc. of the IEEE International Conference on Systems, Man and Cybernetics (SMC '10),* 1953–1957.

APPENDIX: Mathematical Model of LSEA

As mentioned earlier, LSEA algorithm uses a 64-bit key and expands it to generate keys for each round that are used to encrypt data. This appendix presents the mathematical details of key expansion and encryption's procedure. The block of expanding key generates five unique keys using the initial 64-

bits. First, the key of size 64-bit (*Kin*) is divided into 16 smaller segments of 4-bits each. Later, four *f* function blocks work on the data of 16-bit and the initial substitution is performed using

$$Ke = \prod_{i=1}^{4} Kin_{(i-1)+j} \qquad \text{(A-1)}$$

For first four rounds *i*= 1 to 4, the expanded keys (*Ke*) are determined using permutations of the initial input key (*Kin*). Next round will pass the 16-bits of Ke to the *f*-function to further expand the key to (*Kef*) by

$$Kef = f(Ke) \qquad \text{(A-2)}$$

The *f*-function transformation performs linear and non-linear transformations to generate more confusion and diffusion. This will result in four keys (K_1, K_2, K_3 and K_4) while the 5th key (K_5) can be obtained by XOR operation between the four round keys as

$$K_5 = K_1 \oplus K_2 \oplus K_3 \oplus K_4 \qquad \text{(A-3)}$$

Once all keys are obtained, the encryption is started where more data diffusion and confusion can be achieved with extra shift and logical operations. The 16-bit segments are obtained from the 64-bit data represented by M_{0-15}, M_{16-31}, M_{32-47} and M_{48-63}. It is worth to mention that at each round the swapping is applied to increase confusion. Bitwise *XNOR* is applied between the cipher key K_1 and M_{0-15}, K_4 and M_{48-63} to obtain R_{11} and R_{14} respectively in the first round. The result of *XNOR* is fed to the ***f***-function to provide El_1 and Er_1. It is worthy to note that the ***f***-function used here is the same used in key expansions. Bitwise *XOR* is now applied between El_1 and M_{32-47} to attain R_{12} and between Er_1 & M_{16-31} to attain R_{13}. This can be expressed as

$$R_{j,i} = \begin{cases} M_{j,i} \odot K_j & i = 1, 4 \\ M_{j,i+1} \oplus El_j & i = 2 \\ M_{j,i-1} \oplus Er_j & i = 3 \end{cases} \qquad \text{(A-4)}$$

The transformation is constructed in a way that for the next round R_{11} will become M_{16-31}, R_{12} will become M_{0-15}, R_{13} will become M_{48-63} and finally R_{14} will become M_{32-47}. The transformed data segments again encrypted using equation (A-4) with the second key generated from the key expansion. The process is continued for all the five keys. The results of final round are joined to extract the encrypted data ciphertext (*C*) which is given by

$$C = \text{Concatenate}(\mathrm{R}_{51}, R_{52}, R_{53}, R_{54}) \qquad \text{(A-5)}$$